KASPERSKY lab

The benefits and strategic importance of

Kaspersky Security for Internet Gateway

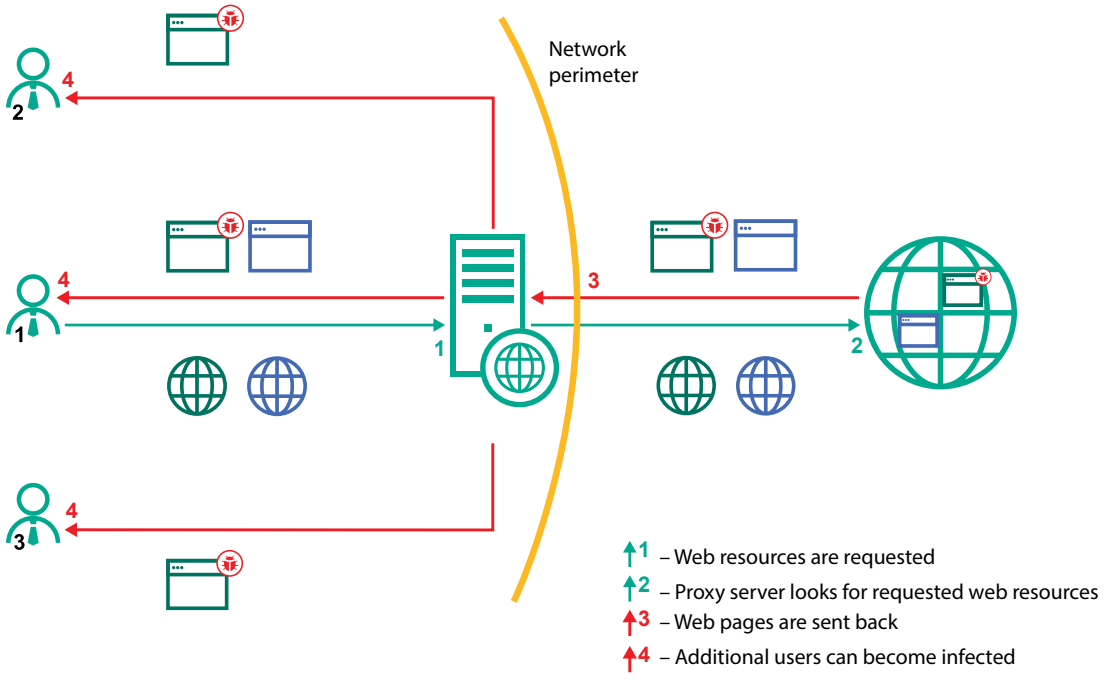
www.kaspersky.com
#truecybersecurity

The benefits and strategic importance of Kaspersky Security for Internet Gateway

A secure gateway remains the first line defense for the majority of corporate security scenarios, despite the penetration of mobility into the working processes. This is not going to change, even as it gives way to its cloud counterpart, the Cloud Security Gateway. As a natural bottleneck for all traffic passing between the corporate infrastructure and the outside world, it offers excellent capabilities for containing threats early and with relatively little effort.

In the concept of layered protection, mitigation of the infection **before** it reaches the endpoint offers considerable reduction of risks, for example:

- At the endpoint level, the human factor is added to the equation, the impact of which is not easy to predict. The clever use of social engineering, especially if the working process doesn't allow for strict security policies, can sidestep even reliable endpoint-based protection. A gateway level security solution would not be affected by this.
- More risk reduction in case of gateway security layer implementation comes out of the typical preparation/testing model for the majority of malware. The attackers specifically research the endpoint, and their evasion tricks are usually focus its specific environment. Endpoint protection is also the easiest to recreate in order to test the malware. But the proxy server protection is considerably different – and the majority of attackers just don't bother with recreation of a gateway defensive system for the sake of testing.
- When the endpoint-based protection successfully blocks the malware, it usually alerts both the user and the administrator. If the attack is a mass one – or the malware has made it into the proxy server's cache – the entire network could start raising alarms on users and admin staff. This situation is likely to disrupt business operations, even more so for smaller businesses that may have a shortage of IT staff and lack a highly developed framework for dealing with these kinds of situations. In this environment, every specialist helpdesk hour adds to the financial strain – this in addition to lost revenues due to the whole disruption. Clearly, blocking the threat at an earlier stage, right at the network's entrance, can save much time and money.
- The last and the simplest: some endpoints, due to the nature of the tasks they're used for, can be deliberately left without any security solutions. Therefore, it's crucial to protect them at the gateway level.



Without gateway protection, infections can spread

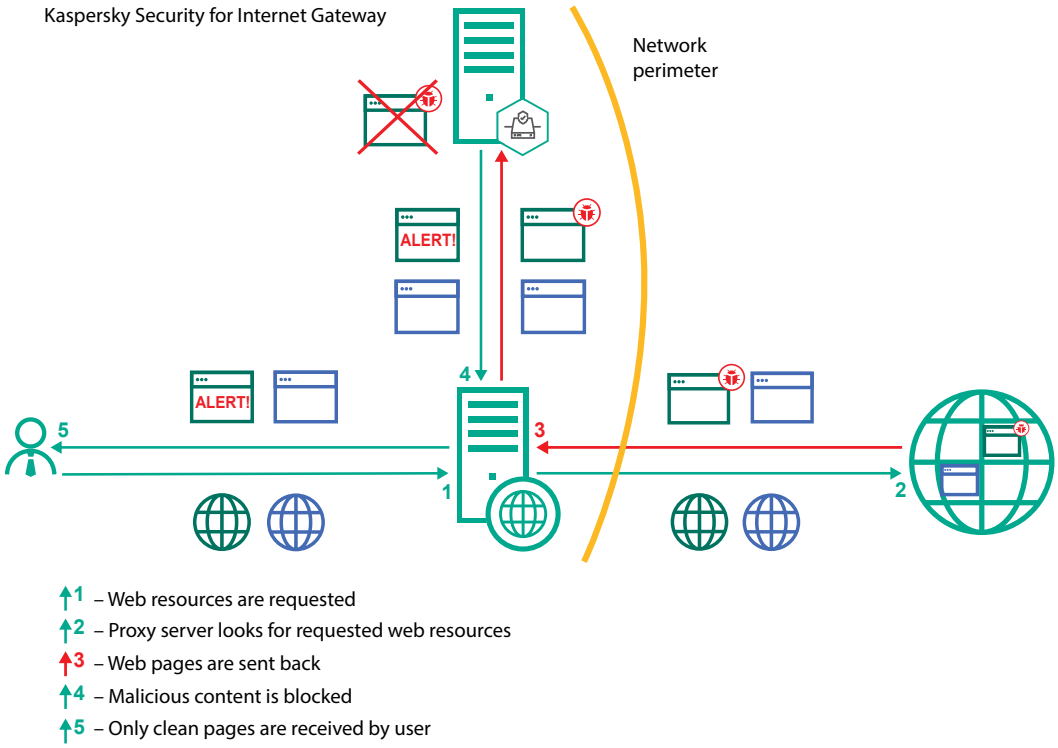
The proxy server is the one of two bottlenecks where incoming threats can be contained at the earliest stage of an attack's killchain (the other being email). The proxy server security solution protects the corporate IT network from the dangers of the World Wide Web, and also increases productivity by governing internet use.

Key features and benefits of Kaspersky Security for Internet Gateway:

- Protection from the majority of modern malware and ransomware. Given the high rate of re-use of older malware, static machine learning-based algorithms and emulative sandboxing filter out **95%** of incoming threats.
- The newest threats are precisely detected without any false positives immediately after their discovery by Kaspersky Lab through Kaspersky Security Network – no waiting for updates.
- The solution's architecture allows for the easy implementation of corporate traffic monitoring (also known as 'SSL bumping'). This controls and secures SSL-encrypted web traffic – essentially the de-facto standard for Internet communications.
- Leverages extensive threat intelligence together with specialized heuristic algorithms to block malicious and phishing websites before the user is threatened.
- For high-load systems, the solution is scalable, allowing for multiple node management and hierarchical deployment.
- Although SMBs may experience targeted attacks less often than large enterprises, they can still be attacked as part of a contractor chain to reach a bigger target. The risk of this kind of attack being successful is reduced considerably by the availability of a targeted attack-related hosts database, constantly updated by renowned Kaspersky Lab APT hunters. And if your business can afford Kaspersky Anti-Targeted Attack (KATA), Kaspersky Security for Internet Gateway can integrate with Kaspersky Anti Targeted Attack as a web sensor, further boosting its detection capabilities can integrate with KATA as a web sensor, further boosting its detection capabilities.
- The transmission of certain file types moving in and out of the network can be restricted by Content Filtering. This reduces the risks of infection and sensitive data leaks.
- Effective Web Control scenarios can be implemented to restrict the use of specific categories of web resources; custom rules can also be created. This helps boost productivity by preventing distractions and also lessens the chances of infection – certain web resources, such as those serving pirated software or illegal content can double as malware websites.
- Good visibility is key to successful incident response. Kaspersky Security for Internet Gateway has broad capabilities that help administrators to react promptly to events requiring their attention. These include a web-based dashboard for event tracking, event-centric threat analysis and integration with existing Security Information Event Management (SIEM) systems.
- For service providers and diversified businesses, the multi-tenancy function facilitates the management of multiple systems from a single console. Each can have their own administrator with role-dependent privileges.
- For companies and institutions operating with highly sensitive data and /or with low tolerance for security incidents, it makes perfect sense to employ Kaspersky Security for Internet Gateway alongside existing web gateway protection. As a powerful additional security layer, Kaspersky Security for Internet Gateway boosts detection rates without generating additional false positives.

Conclusion

The value of forefront protection for any company's security cannot be overestimated. Having every level of your IT network covered with a comprehensive range of security solutions from Kaspersky Lab will keep your business data safe and your business continuity on track.



Kaspersky Security for Internet Gateway blocks threats before they reach the user

Kaspersky Lab
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com